## IN THE CLAIMS

Please amend the claims as follows. Presented below is a complete listing of claims in the revised format showing markings as set forth by the U.S. Patent and Trademark Office on January 31, 2003:

1. (Currently Amended) A method of authenticating a client, the method comprising in an authentication server:

receiving a record ID for a user, and a one-time key generated by the a third party server and encrypted with a user's public key by the server; receiving the user's authentication data from the client;

determining if the user's authentication data matches the record ID; and if so, decrypting the one-time key with the user's private key, and returning the decrypted one-time key to the client.

- 2. (Currently Amended) The method of claim 1, further comprising registering the user with the authentication server, registering comprising: receiving a registration authentication data from the user; generating a random public key/private key pair for the user; generating a random record ID for the user; and associating the authentication data and the private key with the record ID.
  - 3. (Original) The method of claim 2, further comprising: sending the record ID and the public key to the user.

02

- 4. (Currently Amended) The method of claim 2 further comprising establishing a secure connection with between the authentication server and the user, prior to receiving registration authentication data.
- 5. (Currently Amended) The method of claim 1, wherein a web page presented by the <u>third party</u> server to the client prompts the user to enter the authentication data to log in to the server.
- 6. (Original) The method of claim 5, wherein the client's authentication data is automatically redirected to the authentication server.

~~~

- 7. (Original) The method of claim 1, wherein the authentication data is biometric data.
- 8. (Original) The method of claim 1, wherein the authentication data is personal data selected from among the following: a password, a smart card, and another type of authentication card.
- 9. (Currently Amended) The method of claim 1, wherein the client forwards the decrypted one-time key to the <u>third party</u> server, thereby authenticating the user as the owner of the private key.
- 10. (Original) A method of claim 1, further comprising discarding the record ID after returning the one-time key to the user.

003022.P019X 4 09/707,417

- 11. (Original) The method of claim 1, wherein the record ID and the encrypted one-time key are further encrypted using a partner key, the method further comprising decrypting the record ID and encrypted one-time key using the partner key.
- 12. (Original) The method of claim 11, wherein the partner is a symmetric key set up during registration of the partner.
- 13. (Original) The method of claim 11, wherein the partner key is a private key of the authentication server.
- 14. (Currently Amended) A method of using a third party an authentication server to authenticate a user to a third party server, the method comprising the third party server:

looking up a record ID associated with the user;

generating a one-time key and encrypting the one-time key with a public key of the user, and sending the encrypted one-time key and the record ID to the user;

receiving authentication data, the authentication data being the decrypted onetime key <u>decrypted with the user's private key by the authentication server, such that</u>
<u>the user does not have control of the user's private key at any time</u>; and
permitting access to the server.

15. (Original) The method of claim 14, comprising: determining an authentication policy associated with the user; and verifying that the authentication policy has been satisfied, prior to permitting access to the server.

0

16. (Original) The method of claim 15, wherein verifying that the authentication policy has been satisfied comprises:

determining if the server should verify additional data; and
if so, requesting additional data from the user prior to generating the one-time
key.

17. (Currently Amended) A third-party authentication system comprising: an authentication server to receive a record ID for a user, and a one-time key generated by the <u>a third party</u> server and encrypted with a user's public key by the <u>third party</u> server;

a comparison logic in the authentication server to receive user authentication data from the client and determine comparing whether the user's authentication data matches the record ID; and

a decryption logic in the authentication server to decrypt the one-time key with a private key associated with the validated record ID, and returning to return the decrypted one-time key to the client.

18. (Currently Amended) The system of claim 17, further comprising: a policy validation logic to receive a policy from the third party server, and determine if the policy has been fulfilled; and

the decryption logic to decrypt the one-time key only if the policy has been fulfilled.

19. (Original) The system of claim 17, further comprising: a nonce generation logic to generate a nonce, the nonce to be included with the user authentication data from the client; and

~ ()~ the comparison logic to verify that the user authentication data includes the appropriate nonce.

20. (Original) The system of claim 17, further comprising a client registration logic to register the user, the client registration logic comprising:

a key generation logic to generate a random public key/private key pair for the user;

a record ID generation logic to generate a random record ID for the user; and the client registration logic to associate user authentication data with the private key and the record ID.



- 21. (Original) The system of claim 18, further comprising: the interface to send the record ID and the public key to the user.
- 22. (Original) The system of claim 19, wherein the interface establish a secure connection with the user, prior to receiving registration authentication data.
- 23. (Original) The system of claim 17, wherein a web page presented by the server to the client prompts the user to enter the authentication data to log in to the server.
- 24. (Original) The system of claim 23, wherein the client's authentication data is automatically redirected to the authentication server.
- 25. (Original) The system of claim 17, wherein the authentication data is biometric data.

003022.P019X 7 09/707,417

- 26. (Original) The system of claim 17, wherein the authentication data is personal data selected from among the following: a password, a smart card, and another type of authentication card.
- 27. (Original) The system of claim 17, wherein the client forwards the decrypted one-time key to the server, thereby authenticating the user as the owner of the private key.
- 28. (Original) The system of claim 17, further comprising a security mechanism to discard the record ID after returning the one-time key to the user.

() V

- 29. Original) The system of claim 17, wherein the decryption logic further decrypts the record ID and the encrypted one-time key with a partner key.
- 30. Original) The system of claim 29, wherein the partner key is a symmetric key set up during registration of the partner.
- 31. (Original) The system of claim 29, wherein the partner key is a private key of the authentication server.